APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/503,205	02/14/2000	Jun Kogure	826.1590/JDH	6229

21171	7590	05/16/2006

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER
KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)	
Office Action Summary	09/503,205	KOGURE, JUN	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>21 April 2006</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-19</u> is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) <u>1-10</u> is/are allowed.

6)☒ Claim(s) <u>11-19</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All   b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>02/28/06</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____ .

U.S. Patent and Trademark Office

PTOL-326 (Rev. 7-05)   Office Action Summary   Part of Paper No./Mail Date 20060510

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 04/21/06. Applicant amended

Claims 1, 8, 9, 10, 11, and 16. The amendment filed on 04/21/06 have been entered and made of

record. Therefore, presently pending claims are 1-19.

Response to Arguments

Applicant's arguments filed 10/19/05 have been fully considered.

The applicant argues that one of ordinary skill in the art would not look to modify an

apparatus for testing very large scale integrated circuit devices as taught by Eichelberger, in a

manner as the Examiner contends so as "to be as unpredictable as possible." This is not found

persuasive. The passphrase that is disclosed by Schneier is the component of the system that the

examiner considered to be unpredictable. The applicant will not that this value is a key and

therefore, random. A random number is by definition an unpredictable number. As stated in the

combination the system of Leppek would be the system being tested and therefore added to the

system of Eichelberger. The system of Eichelberger employs pseudo random number as a source

of test stimuli. This is so that although the test results should be predictable, the stimuli should

not be limited by the users imagination and therefore random (unpredictable).

The applicant argues further that one of ordinary skill in the art would not look to modify

such a testing apparatus as taught by Eichelberger with PGP algorithms taught by Schneier that

are used for cryptography without the benefit of appellant's specification. This is not found

persuasive. The examiner did not combine the Eichelberger reference with Schneier for the PGP

algorithm. The examiner would like to bring to the applicants attention to the system of Leppek

which includes a PGP algorithm in the selection of algorithms available (description of Fig. 2 in

Leppek 6,868159). The applicant mentioned that during the phone interview the reference was

Leppek (5,933,501). This is the correct inventor, but the wrong patent. The correct patent is

Leppek 6,868,159.

The applicant argues that Leppek teaches a data processing and communications system

where "the present invention resides primarily in what is effectively a prescribed set of

communication encryption and decryption software employed by digital data terminal and

communication equipment." This is not found persuasive. Although the reference is directed to

an entirely different problem than the one addressed by the application, the combination of

references discloses every limitation recited in the claims.

Therefore the motivation provided by the examiner, for the combination of Eichelberger

by adding the system of Leppek as the system to be tested in the system of Eichelberger, is stated

in the Final office action as the system of Eichelberger, which as the applicant mentioned is a

testing system, would be used to test the system of Leppek. Further the system of Eichelberger

can be used to carry out more sophisticated testing techniques (Eichelberger column 2 lines 20-

25).

In reference to applicant's argument that Wright does not teach an irreducible polynomial,

according to an aspect of the present invention, the claim 13 does not recite "an irreducible

polynomial.".

The rejection is therefore maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 11-12 and 14-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Eichelberger et al. (4,687,988) in view of Leppek (6,868,159), and further in view of Schneier

("Applied Cryptography").

In reference to claims 11 and 16 Eichelberger discloses a data generating method,

comprising: a condition that is specified by the user (column 3 lines 22-31); generating a

plurality of random numbers based on the designated condition (column 3 lines 39-40);

generating expression data of the finite field based on the generated random numbers (part 30

Fig. 1); and storing the generated designated expression data (column 3 lines 39-47).

Eichelberger does not disclose designating a condition for a finite field.

Leppek suggests a data generating apparatus and computer readable storage medium,

comprising: an input device inputting a condition for designating a finite field (column 4 lines

33-51).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to use the system of Leppek in the good simulation machine of Eichelberger so

that the random number produced by the pseudo random number generator of Eichelberger so

that the system of Leppek would generate expressions for all the values created by the good

machine and store them in the storage space of Eichelberger. One of ordinary skill in the art

would have been motivated to do this because this would be a method of using the testing system of Eichelberger to test the system of Leppek.

Although Leppek discloses a system that uses PGP (column 4 lines 14-17), Leppek does not provide details that would indicate that the PGP algorithm whose conditions are of a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as prime number and a positive integer indicating an extension degree, respectively. In addition, Leppek is silent on the origins of the key 170 and therefore a condition specified by a user.

Schneier discloses the details of the PGP algorithm (page 584), which includes IDEA. The IDEA algorithm has S-boxes which have the condition are of a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as prime number and a positive integer indicating an extension degree, respectively (page 320 paragraph 2). Schneier discloses the user entering a passphrase that is used as the conditions for the hash algorithm to create the key (page 174 paragraphs 2-7).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use details of the PGP algorithm as disclosed by Schneier and have a user enter the passphrase as disclosed in Schneier to enter the key that is disclosed by Leppek. One of ordinary skill in the art would have been motivated to do this because Leppek does not disclose the details of the PGP algorithm that is used as part of the invention while Schneier gives the details and the user entered passphrase gives the user the ability to be as unpredictable as possible.

Regarding claims 12 and 17, the system of Leppek further comprising an operation

device performing a finite field operation based on the expression data stored in said expression

data storage device (column 5 lines 34-52).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to use the system of Leppek in the good simulation machine of Eichelberger so

that the random number produced by the pseudo random number generator of Eichelberger so

that the system of Leppek would generate expressions for all the values created by the good

machine and store them in the storage space of Eichelberger. One of ordinary skill in the art .

would have been motivated to do this because this would be a method of using the testing system

of Eichelberger to test the system of Leppek.

Regarding claims 14, and 18, wherein when a bit length of a prime number which

describes the finite field is inputted as the condition, said generation device automatically

generates prime number data corresponding to the bit length and stores the generated prime

number data in said expression data storage device. Leppek uses different encryption routines

(column 4 lines 14-17) one well known example is the RSA encryption routine, which uses

random keys. The size of the keys is a design choice. The keys are inherently developed using a

random number generator, which would generate them automatically

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to use the system of Leppek in the good simulation machine of Eichelberger so

that the random number produced by the pseudo random number generator of Eichelberger so

that the system of Leppek would generate expressions for all the values created by the good

machine and store them in the storage space of Eichelberger. One of ordinary skill in the art

would have been motivated to do this because this would be a method of using the testing system

of Eichelberger to test the system of Leppek.

Regarding claims 15 and 19, further comprising: a designation device designating

expression data of a finite field (column 5 lines 6-18); and a verifier device verifying whether the

designated expression data are suitable, the verifier device sores designated expression data in

said expression data storage device if the designated expression data are suitable, and the verifier

device asks the designation device for other expression data if the designated expression data are

not suitable (claim 5 lines 19-33). The supervisory encryption assembly manager processes the

sequence and therefore is responsible for verifying that the encryption process is carried out as

designed.

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to use the system of Leppek in the good simulation machine of Eichelberger so

that the random number produced by the pseudo random number generator of Eichelberger so

that the system of Leppek would generate expressions for all the values created by the good

machine and store them in the storage space of Eichelberger. One of ordinary skill in the art

would have been motivated to do this because this would be a method of using the testing system

of Eichelberger to test the system of Leppek.

Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Eichelberger et

al. (4,687,988) in view of Leppek (6,868,159), and further in view of Schneier ("Applied

Cryptography") as applied to claim 11 above, and further in view of Wright.

Leppek does not expressly disclose the generation of polynomial expressions

Regarding claims 13, Wright discloses a random polynomial generator wherein when an extension degree which describes the finite field is inputted as the condition, said generation device automatically generates irreducible polynomial data corresponding to the extension degree and stores the irreducible polynomial data in said expression data storage device (part 2.1 page 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the polynomial generator as in Wright in the system of Leppek. One of ordinary skill in the art would have been motivated to do this because Leppek discloses the use of conventional encryption algorithms (column 4 lines 14-17) and Wright discloses a polynomial generator which is satisfactory and has already been proven (Introduction 1 page 1).

Allowable Subject Matter

Claims 1-10 are allowed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period
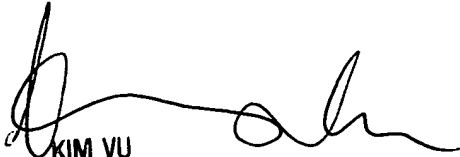
will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854.

The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Thursday, May 11, 2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100